AAMC

Association of
American Medical Colleges
2450 N Street, N.W., Washington, D.C. 20037-1127
T 202 828 0400 F 202 828 1125
www.aamc.org

Testimony of Joanne M. Conroy, MD, Chief Health Care Officer
Association of American Medical Colleges
Before the ONC HIT Standards Committee
November 19, 2009

My name is Joanne M. Conroy. I am an anesthesiologist by training. Currently I service as Chief Health Care Officer of the Association of American Medical Colleges (AAMC). In that role I represent the interests of approximately 400 major teaching hospitals and health systems, including 64 Veterans Affairs medical centers. Prior to coming to the AAMC, I was executive vice president of Atlantic Health System and chief operating officer of Morristown Memorial Hospital in Morristown, New Jersey. As you have requested, I am here today to speak about the views of teaching hospitals and health systems as they face challenges and threats related to data theft, loss, and misuse.

AAMC member teaching hospitals and health systems are large, complex institutions that face challenges beyond those of many smaller hospitals and health systems. These are attributable to a confluence of factors that support their missions--the number of patients they treat; the number of sites—both inpatient and outpatient—at which they provide health care; the number of individuals they employ; the students they train; and the clinical research they conduct. On the one hand, these factors suggest the challenges and complexities faced by academic medical institutions. On the other hand, they have motivated AAMC members frequently to be leaders in taking actions to identify the risks that pose the greatest dangers to the protection of confidential data and minimize them, while at the same time not compromising the quality of care or patient safety.

While there is no typical AAMC member, I can provide you with a representative example. One member employs 10,500 individuals, has an active medical-dental staff of over 1,400 physicians and dentists, trains over 230 residents, and has on its premises approximately 6,500 workstations used by clinical and business staff. In some cases the physicians are employed, in others they are not; they may be volunteers, or they may be community physicians who use the institution's electronic health record on only an occasional basis.

As several members noted, "the diverse nature of the academic medical campus requires these organizations to develop collaborative security plans and mitigation strategies." Commonly the effort involves the IT department and legal/compliance offices. To support these efforts, continuing employee education about data security policies and procedures is essential, as is ensuring that all trainees—including residents, medical, nursing, and other allied health professions students—have the appropriate training. This is particularly challenging given the large number of individuals involved, and that they commonly rotate through numerous sites in the course of their training.

Among the approaches to data theft from internal sources are strong security policies and standards and education programs for employees; teaching employees to encrypt sensitive data and report suspicious activities or possible breaches; providing secure e-mail to employees; requiring two factor authentication for remote access to the network; local encryption of laptops and PDAs; proactive monitoring; logging data use by authorized users; and termination of employment for misuse.

One of the biggest challenges facing AAMC members is the use of portable devices—laptops, PDAs, thumb drives, cell phones—that are brought onto the premises. Students and residents can make this an even bigger issue, as these devices seem to be a critical part of their lives and go with them everywhere. It is hoped that continuing education about the need to value security and confidentiality will ease this problem.

When a theft occurs, institutions take steps to ensure that it will not happen again. If the incident results in a risk of identity theft, then credit monitoring is provided for one year to the individuals whose information was stolen. Many institutions are moving to full disk encryption and encrypted USB drives to mitigate the risks.

Employees who are found to have inappropriately accessed information face a range of disciplinary actions, including termination.

As the Panel's third questions acknowledges, there are trade-offs between security and usability. If access to patient data is too difficult, the result may be that clinicians will not access the information or use it in their clinical decision-making. Patient safety remains the most important consideration, so institutions take an approach that allows them to understand the risk presented by an issue and the mitigations strategies that are available, while still keeping patient safety as the primary consideration.

Finding security solutions that work across platforms often means that AMCs must select more costly solutions. While encryption products have improved, they can still be a barrier unless they are fully integrated with workstation authentication.

Faculty rotate through different hospitals, and often need to access data at Hospital A while working at Hospital B, so hospitals must be creative in negotiating through multiple firewalls. Much attention is paid to security servers.

I already have mentioned the use of encryption. Members also report strategies such as using virtual desktops that are configured to prevent cut and paste, downloading to local machines, and printing outside the institutions. Some institutions scan high-risk areas for confidential data.

Teaching institutions also maintain data that is generated in the course of clinical research, a special security challenge. While the research is on-going, it cannot be de-identified. Once the research is completed, there may be reasons that it must remain in identifiable form. Sometimes there are investigators who, often without the assent of the institution, maintain confidential data in their own databases. This data may be especially vulnerable to breaches and misuse. When users work on data outside the constraints of an institution—as sometimes happens in research—there is no good mechanism to know when someone has moved a confidential file out of the protected server environment.

A frequent complaint is the lack of vendor support, as some vendors do not deliver secure applications.

Interoperable information security standards would be very helpful to our member institutions. Currently, vendors do not adhere to common standards, so it is difficult to implement new applications and to ensure that all applications are secure. It is anticipated that one of the biggest challenges will be implementing standards that will work for both vendor-based and homegrown systems.

As patients move from clinic to hospital and back, and as they move from one healthcare provider to another, the data does not follow easily. IT resource constraints are a major barrier to integration, and information security adds yet another wrinkle.

A unique patient identifier would be a very helpful step toward ensuring data security. It would provide a way to solve the issue of identity management and allow access to the data by appropriate parties, while barring access to those who should not have it.

Some of the emerging issues include: the use of social networking and personal devices; ensuring the security of information placed in health vaults, on memory sticks, and in health information exchanges; the increasing possibility of security breaches as patients gain access to their own EHR and maintain a PHR; cyber threats that will come in through highly advanced phishing scams and vulnerable software applications; and the malicious software downloads that will occur through innocent clicking on web sites.

AAMC members are keenly aware of the advantages of electronic data, but also realize that such data presents many opportunities for theft, loss, and misuse. They are working diligently to minimize these risks and hope to find support for these efforts in government policies that will reduce variations among products and support efforts to improve patient care, while not imposing barriers to physicians and other providers in their roles as clinicians, researchers, teachers, and learners.

Thank you. I look forward to the discussion following this panel.